Department of Homeland Security Daily Open Source Infrastructure Report for 3 December 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- The Associated Press reports that pirates chased and shot at a U.S. cruise liner with more than 1,000 people on board but failed to hijack the vessel as it sailed through the Gulf of Aden on Sunday. (See item **10**)
- According to Stars and Stripes, U.S. Army medical officials in southeast Germany waited nearly two months before notifying more than 6,000 beneficiaries of a possible security breach regarding their personal information stored on a lost laptop computer. (See item **20**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *December 2, St. Louis Post-Dispatch* – (Missouri) **Ameren restores power to 53,000.** Ameren crews have restored power to all of the 53,000 customers who lost it Tuesday morning after a small fire started near a transformer. “The smoke and heat caused the transformers and other equipment to switch off because it was so intense,” said Ameren’s spokeswoman. The transformer itself had smoke damage but was not on fire, she said. At its peak of the outage — from about 4:30 to 6 a.m. Tuesday — customers from Clayton to Interstate 55 in south St. Louis County were in the dark. Within about three hours, Ameren crews had restored power. The problem began about 4:30 a.m. when a fire started next to a transformer at the Watson substation. The Shrewsbury Fire chief said an Ameren employee quickly put out the fire using a handheld extinguisher.

Ameren's spokeswoman said this about the cause of the fire: "We know there was an oil can there and it ignited, but we don't really know other than that."
Source:
http://www.stltoday.com/stltoday/news/stories.nsf/0/27F596B1059F964186257513004 16F12?OpenDocument

2. *December 2, Reuters* – (California) **Exxon says LA refinery output cut on shutdown.** Exxon Mobil Corp said production at its 150,000 barrel per day Los Angeles-area refinery in Torrance, California, would be cut by an undisclosed amount following a unit shutdown during the morning of December 1. "We do anticipate some impact to production from Monday's event," said an Exxon spokeswoman. "Unfortunately I won't be able to get into specifics." Exxon has also declined to disclose which unit at the Torrance refinery had to be shut after malfunctioning. The spokeswoman did say the unit was completely shut and not on standby, which allows for a quicker restart.
Source: http://www.reuters.com/article/rbssEnergyNews/idUSN0253599220081202

3. *December 1, Idaho Business Review* – (National) **Girding up for plug-ins: Groups seek power system management.** Another major source of demand is on the horizon: plug-in hybrid electric vehicles (PHEVs). The current. President-elect has already expressed his support for expanding the nation's fleet of PHEVs, calling for a million of them on the road by 2015, and a $7,500 tax credit for the purchase of plug-ins is already on the books. As the Northwest Power and Conservation Council prepares to draft its next Northwest Power Plan, officials are taking a look at the potential impacts of plug-ins on the regional grid. "…Down the line, as you grow the number (of plug-ins) there's going to have to be some kind of charging regulation," said the council chairman. Council members met late last month to hash out the benefits and challenges of bringing PHEVs onto the grid, taking in a presentation from a Battelle Pacific Northwest Laboratory scientist. He has been working for two years on research into "smart-grid" technology which incorporates sophisticated tools that allow PHEVs to communicate with the power grid, drawing from it during low-demand times and potentially giving back to it — or shutting off — during peaks. His research suggests that by using smart-grid management, between 43 and 73 percent of all the cars and trucks in the United States could be replaced with PHEVs without requiring new power plants or transmission lines.
Source: http://www.idahobusiness.net/archive.htm/2008/12/01/Girding-up-for-plugins-Groups-seek-power-system-management

4. *December 1, Pittsburgh Tribune-Review* – (Pennsylvania) **Valve failure injures natural gas worker.** A worker in Washington County, Pennsylvania, was injured Sunday when a natural gas line inlet valve failed, causing the release of natural gas and a loud boom. Workers at MarkWest Energy's Chartiers plant were "pigging" a line Sunday when the valve failed, the plant manager said. "Pigging" uses pipeline inspection gauges to perform various maintenance functions in a pipeline without stopping the flow of natural gas. There was no explosion. The worker hit his head after the valve failure and was treated at a local hospital, MarkWest officials said. Plant workers isolated the gas line immediately, the plant manager said. It will continue to be

isolated until the manufacturers of the equipment are able to identify what went wrong. The plant will be closed until the cause of the failure is determined, said the plant's environmental health and safety coordinator. The natural gas processing plant opened October 20, as part of MarkWest Energy's first venture into Pennsylvania, the plant manager said.
Source: http://www.istockanalyst.com/article/viewiStockNews+articleid_2845002.html

5. *December 1, Putnam County Sentinel* – (Ohio) **Lima Post investigating commercial tanker explosion.** A tanker carrying 8,500 gallons of gasoline was northbound on Ohio 65 when it overturned. The tanker, owned by Ottawa Oil Company, rolled, struck several utility poles, and caught fire. As a result of the crash, the Cairo station of American Electric Power was affected, causing power outages to over 1000 area residents. The patrol's investigation is ongoing.
Source:
http://putnamsentinel.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=4403&TM=61013.3

[Return to top]

Chemical Industry Sector

6. *November 30, WHIO 7 Dayton* – (Ohio) **Darke Co. authorities respond to 2 bomb threats.** The dispatch center at the Darke County Sheriff's Office received two telephone bomb threats minutes apart late Sunday night. The first call came in at about 10:50 p.m. stating that the caller placed four bombs at the Anderson-Marathon Ethanol Plant at the east edge of Greenville. The plant began production of corn-based ethanol in February of this year. It is located in the new Greenville Industrial Park off State Route East 571. Minutes later the caller, believed to be the same caller, made a second phone call to Darke County 911 Center claiming to have also placed bombs at the Wal-Mart Superstore at 1501 Wagner Avenue in Greenville.
Source: http://www.whiotv.com/news/18176152/detail.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *December 1, Associated Press* – (Michigan) **AEP nuclear plant in Michigan may not be back on line fully until 2010 at cost of $332 million.** American Electric Power Co. (AEP), one of the nation's largest power generators, said Monday that a unit at one of its nuclear power plants damaged in September will not return to full service until 2010. The company also estimated the cost at repairing and replacing the damaged turbine rotors in Cook Nuclear Plant's Unit 1 at $332 million. AEP figures to recover most of the cost through insurance and warranties. The unit at the plant in Bridgman, Michigan, has been out of service since September 20 after severe turbine vibrations damaged the main turbine and generator. Under the company's best-case scenario, the company estimates the unit can be returned to service by September, but with an approximate power reduction of 100 to 250 megawatts from the unit's net capacity of

1,030 megawatts. If repairs are not successful and the unit cannot be restarted until new rotors are available, AEP said the unit will not be back online until 2010.
Source:
http://money.cnn.com/news/newsfeeds/articles/apwire/f60ccdc43e46980e83737fe4d2cca752.htm

[Return to top]

Defense Industrial Base Sector

8. *December 1, Air Force Times* – (National) **Laser fired from nose of 747 for first time.** For the first time, the Air Force test fired the high-energy airborne laser it is developing to shoot down missiles, program officials announced Monday. During the November 24 ground test at Edwards Air Force Base, California, the laser blazed through the beam control/fire control system before shooting out the turret mounted on the nose of a Boeing 747. The beam control/fire control system, operated by a crew inside the jet, steered and focused the beam onto a simulated ballistic missile target. "With the achievement ... the team has now completed the two major milestones it hoped to accomplish in 2008, keeping Airborne Laser (ABL) on track to conduct the missile shoot-down demonstration planned for next year," said the vice president and general manager of Boeing Missile Defense Systems. The ABL aircraft, designated YAL-1A by the Air Force, is a modified Boeing 747-400F whose back half holds the high-energy laser, designed and built by Northrop Grumman. The front section of the aircraft contains the beam control/fire control system, developed by Lockheed Martin, and the battle management system, provided by Boeing.
Source: http://www.defensetech.org/archives/004563.html

[Return to top]

Banking and Finance Sector

9. *December 1, South Florida Sun-Sentinel* – (National) **Theft of children's identities often goes unnoticed for years.** The Federal Trade Commission estimates about 500,000 identity theft incidents annually involve children under age 19, with the majority of the thefts occurring between birth and age 5. That is about 5 percent of all suspected ID theft cases. Federal officials said they have seen the numbers rise slightly during the past several years. Often, but not always, a parent or guardian is involved. The nonprofit Identity Theft Resource Center in San Diego estimates more than half of the child ID theft reports it has examined involve parents or family members. But strangers also can pick up a Social Security number, which has no age identifier, from pediatric or school records, from stolen ID cards, or through data breaches, said the center founder. Some law enforcement agencies also think child ID theft is becoming more attractive to thieves as personal information becomes harder to steal from adults, who are becoming more vigilant about monitoring their credit. A spokesman for the Federal Bureau of Investigation in Washington, D.C., said a "world of financial hurt" can happen between the time a theft occurs and when it is discovered. Often, that gap is a decade or more — when the victim applies for a school loan, a credit card, or a job.

Source: http://www.sun-sentinel.com/business/custom/consumer/sfl-flhlpchildid1201sbdec01,0,2019230.story

[Return to top]

Transportation Sector

10. *December 2, Associated Press* – (International) **Pirates fire on U.S. cruise ship in hijack attempt.** Pirates chased and shot at a U.S. cruise liner with more than 1,000 people on board but failed to hijack the vessel as it sailed along a corridor patrolled by international warships, a maritime official said Tuesday. The liner, carrying 656 international passengers and 399 crew members, was sailing through the Gulf of Aden on Sunday when it encountered six bandits in two speedboats, said the head of the International Maritime Bureau's piracy reporting center in Malaysia. The pirates fired at the passenger liner but the larger boat was faster than the pirates' vessels. The U.S. Navy's 5th Fleet, based in Bahrain, said it was aware of the failed hijacking but had no further details. Ship owner Oceania Cruises Inc. identified the vessel as the M/S Nautica. In a statement on its Web site, the company said pirates fired eight rifle shots at the liner, but that the ship's captain increased speed and managed to outrun the skiffs. All passengers and crew are safe, and there was no damage to the vessel, it said. International warships patrol the area and have created a security corridor in the region under a U.S.-led initiative, but the attacks have not abated.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5gB7YMEDuCwwY9ncDOtPAkEI4-H2wD94QKL7O0

11. *December 1, KMPH 26 Fresno* – (California) **Plane crashes near Coalinga airport.** At around 8:30 pm, a 911 caller reported a small airplane crash near the Coalinga Airport. Fresno County Fire, Fresno County Sheriff, CAL FIRE, the Coalinga City Fire Department, and EMS searched the area for plane wreckage. Foggy conditions delayed discovery of the crash site for an hour, until fire crews found the plane 2 miles north of the airport in a field. Three injured victims were found at the crash site and taken by ambulance to the hospital, with one in critical condition.
Source: http://www.kmph.com/Global/story.asp?S=9434805&nav=menu612_2

12. *December 1, Tulsa World* – (Oklahoma) **Plane carrying Inhofe makes emergency landing.** An American Eagle regional jet carrying 53 people was forced to make an emergency landing Monday after one of its tires was damaged upon take off. None of the 50 passengers and three crew members on board the plane bound for Chicago reported any injuries, authorities said. When the plane took off, a right main gear tire separated and the pilot notified the tower of the problem. The aircraft was then directed to enter a fuel burn-off flight pattern, and later landed safely.
Source:
http://www.tulsaworld.com/news/article.aspx?subjectid=11&articleid=20081201_11_0_AnAmer516019

[Return to top]

Postal and Shipping Sector

13. *December 1, Arizona Republic* – (Arizona) **White powder discovered in Peoria City Hall mailroom.** A white, powdery substance found in a letter at Peoria City Hall was being tested Monday afternoon. Two mail clerks at the facility discovered the substance in an envelope just before noon. The mail room area was cordoned off and the substance was sent to a state lab for testing said a spokesman for the Peoria Police and Fire departments. He said test results should be in sometime Tuesday. A letter of some kind was included with the substance, he said, but because it could not be handled, he did not know exactly what it said.
Source: http://www.azcentral.com/news/articles/2008/12/01/20081201gl-peopowder1201-ON.html

[Return to top]

Agriculture and Food Sector

14. *December 1, Associated Press* – (Michigan) **2 Mich. counties dropped from bovine TB risk zone.** Areas in two Michigan counties no longer are considered potential high risk zones for bovine tuberculosis in livestock. The state Department of Agriculture announced Monday it's dropping high risk designations for the zones in Iosco and Shiawassee counties. The move comes after animal testing in the areas over the last several months revealed no bovine tuberculosis cases. The Shiawassee County area is 100 miles south of the northern Lower Peninsula zone where bovine tuberculosis cases have been concentrated in Michigan. The Iosco County areas are on the border and just south of the bovine TB area. The Shiawassee and Iosco county regions came under scrutiny after bovine TB was confirmed in a couple of deer there in 2007.
Source: http://www.chicagotribune.com/news/chi-ap-mi-bovinetuberculosi,0,6595308.story

[Return to top]

Water Sector

15. *December 2, San Francisco Chronicle* – (California) **Group wants chemical-filled farmland retired.** The giant state and federal pumps in the Sacramento-San Joaquin Delta that funnel water to 25 million Californians should be shut down until certain Central Valley farmers retire hundreds of thousands of acres of chemical-laden farmland, according to a lawsuit filed today by a state water watchdog. Irrigating agricultural land in the western San Joaquin Valley tainted with selenium, mercury, boron, and other toxic substances constitutes an unreasonable use of a public resource protected by state laws and has contributed to the sharp decline of endangered fish species, said the California Water Impact Network (C-WIN). "We think there is a simple solution to California's water problems - to retire all of the drainage-impaired lands in the Central Valley. A second is water conservation - agriculture uses 80 percent of the developed surface water," said the president and founder of C-WIN. The lawsuit marks the latest twist in the continuing Delta drama. The hub of the state's

1,300-square-mile water system is also at the heart of the fight between uses for food and human needs, and those of wildlife and rare plants. In recent years, failure of the ecosystem forced legal rulings that curbed water exports — a move made more complicated this year by a drought and fears of another dry winter. Much of the water has gone to watering cropland laden with chemicals that filter into the San Joaquin River and back to the southern Delta. To date, about 100,000 agricultural acres have been taken out of production due to poor drainage and chemical saturation, said a spokeswoman of the Westlands Water District, which serves 600,000 acres and about 700 farms.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/12/01/BAOH14FHR2.DTL

16. *November 30, Grand Rapids Press* – (Michigan) **Security lapse at Grand Haven power plant prompts review.** The Grand Rapids Water Department director says it should not have taken a full week before she found out about a security breach at a Lakeshore power plant. On September 12, police arrested a man wearing all-black clothing after he sneaked onto the grounds of the Grand Haven Board of Light and Power plant. "We got a call from a neighboring water plant," the director said. The incident occurred 7 miles away from the city's Lake Michigan Water Filtration Plant. The Grand Rapids Water Department director and the protective security adviser for the U.S. Department of Homeland Security for outstate Michigan are hosting a December 11 meeting and have invited utility and law enforcement officials in Kent, Ottawa, and Muskegon counties. Their goal is to make law enforcement aware of the security procedures at facilities that could be considered possible terrorism targets. In Grand Rapids' case, the water filtration plant has had vulnerability assessments and developed round-the-clock security plans, the director said. The adviser said next month's meeting should prevent similar security lapses at local water and power producing facilities. "We're going to establish a security network," he said. "If something suspicious happens at one plant, it's feasible to think it might affect some of the other plants in the area." He said he hopes to create a consortium of utilities that span the entire Lake Michigan coastline.
Source: http://www.mlive.com/grpress/news/index.ssf/2008/11/security_lapse_at_grand_haven.html

[Return to top]

Public Health and Healthcare Sector

17. *December 2, USAgNet* – (National) **Mad Cow variant may be transmissible to humans.** The classical form of mad cow disease and a variant manifest themselves differently, but research suggests that the variant may also be transmissible to humans, according a researcher speaking at Kansas State University. The researcher presented "BSE and BASE: An Update" at the Emerging Infections: A Tribute to the One Medicine, One Health Concept, last month at K-State, reports the Kansas Cattlemen's Association. The presentation addressed studies to assess whether bovine amyloidotic spongiform encephalopathy, often called BASE, is caused by a transmissible prion

strain different from the one that causes classical bovine spongiform encephalopathy or BSE. She said that BASE and BSE differed in several ways, including incubation time. Data suggest that BASE has at least the same animal and human health risks as classical BSE, she said. In September, the Regents Distinguished Professor of Diagnostic Medicine/Pathobiology at K-State and Kansas Bioscience Authority Eminent Scholar with a colleague from the National Veterinary Services Laboratories in Ames, Iowa, published research findings that showed a genetic mutation can cause bovine spongiform encephalopathy - also called BSE or mad cow disease.
Source: http://www.usagnet.com/story-national.php?Id=2802&yr=2008

18. *December 1, Dolan Media Newswires* – (National) **Hospital infections spread, so do lawsuits.** Medical malpractice lawsuits based on hospital infections are on the rise, according to Wisconsin Law Journal. The Centers for Disease Control and Prevention (CDC) in Atlanta has estimated that over 2 million hospital-acquired infections occur annually, resulting in 90,000 deaths. In long-term care facilities, the CDC estimates an additional 1.5 million health-care associated infections occur each year. According to the founder and chair of the Committee to Reduce Infection Deaths, a non-profit patient safety organization in New York, 26 states have passed laws requiring reporting of hospital-acquired infections. Plaintiffs' attorneys say that hospitals can no longer argue that these infections are inevitable.
Source: http://wislawjournal.com/article.cfm/2008/12/01/Hospital-infections-spread-so-do-lawsuits

[Return to top]

Government Facilities Sector

19. *December 2, Local* – (International) **Police clear suspicious parcel from U.S. Embassy.** Police bomb disposal experts have safely removed a suspicious package from the grounds of the U.S. Embassy in Stockholm, Sweden. Police said the embassy had requested them to take care of the package, which arrived on Tuesday morning, although there was no indication of a specific threat. "The Embassy received a suspicious package and our security team took appropriate action by alerting the Swedish authorities," an embassy spokesperson said. "We believe the situation is under control and appreciate the quick response by the police."
Source: http://www.thelocal.se/16070/20081202/

20. *December 2, Stars and Stripes* – (National) **Army waited to tell of possible security breach.** U.S. Army medical officials in southeast Germany waited nearly two months before notifying more than 6,000 beneficiaries of a possible security breach regarding their personal information stored on a lost laptop computer. Authorities know the names, Social Security numbers, and health information of at least 26 individuals were stored on the laptop, according to a news release sent Monday from the U.S. Army Medical Department Activity, Bavaria. However, officials said similar information on approximately 6,000 other patients also may have been on the missing computer, though they do not know for sure. According to the release, the laptop went missing on October 4. Notices that were sent to the beneficiaries on November 24 were

characterized as a precaution. The letters were addressed to not only beneficiaries in the affected region, but to potentially affected people from other regional commands in the U.S. and elsewhere. The release did not explain why Army medical officials waited to notify the public.
Source: http://www.stripes.com/article.asp?section=104&article=59159&source=rss

21. *December 1, Chronicle of Higher Education* – (California) **Extremist foes of animal research torch vehicles near UCLA.** In the latest incident of violence against animal researchers at the University of California at Los Angeles, an extremist group has claimed responsibility for torching two vehicles belonging to an individual who lives near a UCLA researcher but is otherwise unaffiliated with the university. A statement issued by the university denounces the attack and explains that the victim was apparently a mistaken target. A string of recent attacks against the homes and property of animal researchers has led some people to conclude that extremists are shifting their focus away from laboratories and becoming more aggressive in their attacks.
Source: http://chronicle.com/news/article/5580/extremist-foes-of-animal-research-torch-vehicles-near-ucla

22. *December 1, Atlanta Journal-Constitution* – (Georgia) **Package found at federal building was harmless.** A suspicious package found Monday morning at the Sam Nunn Federal Center in downtown Atlanta turned out to be harmless, police said. The package was taken by a bomb squad to a remote location and deliberately detonated by police, an Atlanta police spokesman said. No evidence of explosives was found in the remnants of the package. The Five Points MARTA station and some surrounding downtown streets were shut down for more than three hours Monday morning after a security guard found the package and a bomb-sniffing dog indicated that it might contain explosives. The first floor of the federal center and some nearby businesses were also evacuated. Streets were re-opened about 10:20 a.m. after a bomb disposal removed the package.
Source:
http://www.ajc.com/services/content/metro/atlanta/stories/2008/12/01/atlanta_downtown_package.html

[Return to top]

Emergency Services Sector

23. *December 1, Dallas Morning News* – (Texas) **Dallas Fire-Rescue to test changes in medical emergency response.** A Dallas Fire-Rescue pilot project that eventually could overhaul how the stretched-thin department responds to medical emergencies is scheduled to start January 1. Fire officials believe that the 90-day, $484,000 program — primarily focused on the city's southern sector — will reduce response times, save money and improve the medical service provided to patients. Currently, when a person calls 911 with a medical emergency, an ambulance is dispatched regardless of the severity of the call. Under the new program, the department would still send emergency medical personnel to minor calls in those areas, but they would not be able to take the patient to the hospital, according to a briefing presented Monday to the Dallas City

Council's public safety committee. If the pilot program is successful, fire officials plan to ask the city for additional funding to expand it. Fire officials say they are trying to meet the changing demands of the community. Roughly, six out of 10 of the department's calls are for medical help, and under the current system, a patient with a stubbed toe is given the same priority as someone having a stroke.
Source: http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/120208dnmetfirerescue.1f8c5343.html

24. *December 1, El Dorado Times* – (Kansas) **AT&T agreement will improve 911 system.** Butler County, Kansas, will be making some improvements to its 911 system with an agreement with AT&T. The proposed agreement was presented to the Butler County Commission Tuesday. "What we're asking for is authorization to sign an agreement with AT&T to get copies (of area addresses and phone numbers)," said the county 911 director. The county would receive CDs of data, known as the master street addressing guide. "It is all the 911 data AT&T has for the all of the phone customers in our jurisdiction," the county 911 director said. That information would display the name and address of a person when someone calls. This was attempted in the past, but AT&T had resisted releasing the information because they were concerned it could end up with telemarketers.
Source: http://www.eldoradotimes.com/news/x541371955/AT-T-agreement-will-improve-911-system

[Return to top]

Information Technology

25. *December 2, Heise Security* – (International) **Email Trojans threaten to block email accounts.** A new wave of trojans is rolling through the net. This time, the emails bearing the Trojan warn that the recipient's email account will be blocked within a few hours, they read: "Subject: The email address xyz@heise-online.co.uk is being blocked. Ladies and Gentlemen, due to misuse, your email address "xyz@heise-online.co.uk" will be blocked within the next 24 hours. We have received 98 complaints of spam being sent from it. Details and possible ways to unblock your account can be found in the attachment." The subject and text contain the recipient's address, though the wording and the number of alleged complaints varies. The attached zip file contains the executable file blocking.exe along with the malicious program. These emails should be deleted unread, because most virus scanners are powerless to deal with them. Only a few such programs can currently recognize the culprit. Sophos calls it Mal/EncPk-GH, Microsoft knows it as Win32/Emold.C or Win32/Obfuscator.CT, depending on the mutation, while FProt says it is W32/Trojan3.MX. An analysis by Heise Security has shown that the malware installs itself as the default debugger for the Explorer.exe process, so that it is activated after a reboot. This unusual self-starting mechanism has already been used by the "account-rendered" Trojan, which appeared in users' inboxes exactly a week ago, claiming to be an invoice, a collection order, or a warning of non-payment.
Source: http://www.heise-online.co.uk/security/Email-Trojans-threaten-to-block-email-

accounts--/news/112120

26. *December 2, IDG News Service* – (International) **Apple quietly recommends using antivirus software.** Apple, which has long perpetuated the belief that its operating system is immune to security problems, is recommending that users install security software to make it harder for hackers to target its platform. "Apple encourages the widespread use of multiple antivirus utilities so that virus programmers have more than one application to circumvent, thus making the whole virus writing process more difficult," according to a support note posted last month. Data by computer security researchers has shown that while Apple has not been affected by malicious software nearly to the extent as Windows, it is merely because hackers go after the most widely used platform. Apple is gaining market share, however, which means hackers could increasingly look to exploit the platform, particularly if it becomes perceived as an easier target. Apple systems are also not immune from problems in third-party software, such as plug-ins, which are used to view animated Flash graphics and PDF (Portable Document Format) files. Security problems in plug-ins have frequently been manipulated to cause browsers to redirect to malicious Web sites, which are rigged to try and take advantage of browser flaws. Compared to Windows, there are not nearly as many antivirus products for Apple computers.
Source:
http://www.pcworld.com/businesscenter/article/154760/apple_quietly_recommends_using_antivirus_software.html

27. *December 1, Computerworld* – (International) **New Windows worm builds massive botnet.** The worm exploiting a critical Windows bug that Microsoft Corp. patched with an emergency fix in late October is being used to build a new botnet, a security researcher said December 1. A senior research engineer with Trend Micro Inc., said that the worm, which his company has dubbed "Downad.a" — it is called "Conficker.a" by Microsoft and "Downadup" by Symantec Corp. — is a key component in a new botnet that criminals are creating. Last week, Microsoft warned that the worm was behind a spike in exploits of a bug in the Windows Server service, which is used by the operating system to connect to network file and print servers. Microsoft patched the service with an emergency fix it issued October 23, shortly after it discovered a small number of infected PCs in Southeast Asia. However, the new worm is a global threat, said the senior researcher. "This has real potential to do damage," he said. Trend Micro has spotted infected IP addresses on the networks of Internet service providers (ISPs) in the United States, China, India, the Middle East, Europe, and Latin America. The worm first appeared about a week and a half ago, and began spreading in earnest just before Thanksgiving, he added. He also said that it appears the botnet is being built by a new group of cyber-criminals, not one of the gangs that lost control of compromised computers when McColo Corp., a California hosting company, was yanked off the Internet.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9121958&intsrc=hm_list

28. *December 1, CSO Online* – (International) **The myth of cloud computing.** Virtualization can save money — and open up new security issues. The idea of reducing racks of servers into smaller and cheaper machine farms is simply irresistible in just about every enterprise. Security vendors have seized on this with an array of products promising "security in the cloud." But the adopters often lack a basic understanding of what virtualization is about, and that is a problem, industry experts say. Depending on who you are and where you are, the definition of what is coming in the virtualization world means a lot of different things to a lot of different people, which makes it near impossible to build a security strategy around it. Though many companies do not understand the precise workings of the technology, many at least acknowledge that there is a security challenge to address. The CMO for security vendor Sourcefire, maker of the popular Snort open-source IDS tool, says customers are expressing concern that they have no way to proactively track or identify new virtual systems within their environments. Of course, security experts warn, all the vendor activity in the world would not help a company that dives headlong into the cloud without thinking through the risks first. As long as companies fail to grasp the nuts and bolts of virtualization, dangers remain.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9121923&taxonomyId=17&pageNumber=1

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

29. *December 1, Associated Press* – (National) **Regulators hang up on cell tower backup rules.** Federal regulators have rejected proposed changes by the Federal Communications Commission that would require all U.S. cell phone towers to have at least eight hours of backup power. The White House Office of Management and Budget said late Friday that the FCC failed to get public comment before passing the regulations last year and did not show that the information required from wireless companies would actually be useful. It also said the FCC had not demonstrated that it had enough staff to analyze the hundreds of thousands of pages of documents that the wireless industry said its members would likely have to produce as part of the regulations. A federal appeals court put the rules on hold this summer pending a review by the OMB, which is tasked with overseeing federal regulations.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/12/01/AR2008120102440.html

[Return to top]

Commercial Facilities Sector

30. *December 1, WHAG 25 Hagerstown* – (Maryland) **Chemical spill shuts down Frederick block, bomb squad called in.** A chemical spill shut down several roads in Frederick for more than four hours Monday afternoon. Investigators say the chemical was a liquid when it was spilled, and as a liquid it is stable. But then it turned into a solid, and they say that is what made the chemical highly explosive. The block surrounding the building at 4539 Metropolitan Court was evacuated for about four hours as the Frederick County Hazardous Incident Response Team went in. The block re-opened around 4:30 p.m. NBC25 spoke with employees who worked in the building, and they said a tenant who was renting space in the building was moving out when they accidentally spilled the liquid.
Source: http://your4state.com/content/fulltext/?cid=42371

[Return to top]

National Monuments & Icons Sector

31. *December 1, KSBY 6 Santa Barbara* – (California) **Eight banned from national forests after Gap, Chalk, and Indians fires.** Eight Santa Barbara County residents are banned from all national forests for a year after pleading guilty to violating fire restrictions in the Los Padres National Forest. Five of them pleaded guilty to starting illegal campfires in two different campgrounds. The others pleaded to illegal target shooting. Both have been banned thanks to increased restrictions in the wake of the Gap, Chalk, and Indians fires.
Source: http://www.ksby.com/Global/story.asp?S=9441133

32. *December 1, Baltimore Examiner* – (Colorado) **Feds: Prairie dog no barrier to drilling on refuge.** Federal officials say energy exploration on a southern Colorado wildlife refuge won't have significant environmental effects, despite the presence of a prairie dog deemed eligible for federal protection. The U.S. Fish and Wildlife Service said Monday that an analysis of the Gunnison's prairie dog didn't change its decision that drilling two exploratory wells on the Baca National Wildlife Refuge would have no significant environmental impacts. Environmentalists oppose plans by Toronto-based Lexam Explorations to drill two exploratory natural gas wells on the wildlife refuge next to the Great Sand Dunes National Park. They are concerned about the effects on wildlife, air and water quality, and on the national park. Baca National Wildlife Refuge was created in 2004 with the acquisition of the 97,000-acre Baca Ranch. Some 31,000 acres of that ranch became part of the Great Sand Dunes National Park, previously a national monument, and the rest became the wildlife refuge.
Source: http://www.examiner.com/a-1720124~Feds__Prairie_dog_no_barrier_to_drilling_on_refuge.html

33. *December 1, National Parks Traveler* – (Pennsylvania) **Lawsuit filed over museum complex approved near Valley Forge National Historical Park.** A lawsuit has been filed in a bid to halt a museum complex from being built on 78 acres surrounded on three sides by Valley Forge National Historical Park. The National Parks Conservation

Association (NPCA) and residents from the town of Lower Providence Township, Pennsylvania brought the suit. The filing argues that township planners approved an unlawful zoning ordinance to permit the American Revolution Center (ARC) to build the complex, which is designed to feature a hotel and restaurant along with the museum. The appeal filed by NPCA and Lower Providence residents asserts that the local zoning ordinance is preempted by federal law because it would interfere with and undermine the National Park Service's role in managing the national historical park. The appeal also claims the ordinance is spot zoning, which is illegal under Pennsylvania law, and permits development that is inconsistent and incompatible with neighboring national parkland and other open space. ARC's project has also been opposed by Valley Forge officials as well as the Coalition of National Park Service Retirees.
Source: http://www.nationalparkstraveler.com/2008/12/lawsuit-filed-over-museum-complex-approved-near-valley-forge-national-historical-park

[Return to top]

Dams Sector

34. *December 2, Suburban Journals* – (Missouri) **Levee repairs to begin soon.** Repair work on several St. Charles County levees damaged by heavy flooding during the summer and early fall is set to begin soon. Representatives of several county levee districts are in the process of signing contracts with the U.S. Army Corps of Engineers to fix damage caused by the summer floods and the remnants of Hurricane Ike in September. Mississippi River floodwater breached the 2-mile-long Elm Point levee, near Highway 370 in St. Charles, early in the morning of June 24 despite feverish attempts by volunteers to save it. Water poured through and overtopped the levee. The levee stretches from Huster Road to Danford Creek and protects farm land, businesses, and a sod farm. Some areas do not require total repair, said one of the board members for the Elm Point Levee District. But at least a mile of levee will need to be fixed. The repairs to the Elm Point Levee will cost about $1 million, 80 percent of which is covered by the federal government. The levee district would pay the remaining 20 percent, according to a U.S. Army Corps of Engineers spokesman. The repairs will bring the levee back to its same level, which protected against a flood with a 4 percent likelihood of occurring in a given year, he said. Contractors will take about 90 days to repair a levee by adding clay and dirt 6 inches at a time. After that is completed, they will have to sew grass seeds that have extra-long root systems. The goal is to restore flood protection by the spring flooding season, he said, but repairs could be delayed by ice and snow. The Darst Bottom Levee District also is seeking repairs. Repairs to agricultural levees might be done quicker since the St. Charles County Council November 24 passed a bill exempting existing agricultural levees from requirements for land disturbance and flood plain development permits.
Source:
http://suburbanjournals.stltoday.com/articles/2008/12/02/stcharles/news/1203stc-levee0.txt

35. *December 2, Reno Gazette-Journal* – (Nevada) **Martis Dam opens despite uncertain**

future. Martis Creek Dam was reopened to the public last month, although the U.S. Army Corps of Engineers said earthquake faults and seepage could lead to further repairs or even the removal of the dam. The Corps discovered two earthquake faults near the dam in Martis Valley between Truckee and north Lake Tahoe. They were discovered in two trenches the Corps dug this fall on Waddle Ranch. Coarse soil interfered with fixing the date of the last quake, so more trenches are likely to be dug. Corps officials are worried that if the dam were to fail while holding back a full reservoir that "maximum flooding" could inundate the Martis Valley and downstream communities, including Reno. The Corps has already lowered Martis Creek Lake to reduce seepage. Martis Creek is the only one of several dams in the Truckee-Tahoe area that is managed by the Army Corps of Engineers. Only five of the Corps' 610 dams nationwide are considered more likely to fail. At Martis, previous aerial photography and continuing soil tests will be analyzed in about two months.
Source: http://www.rgj.com/article/20081202/TT/812020323/1047

36. *December 2, Standard Examiner* – (Utah) **Dam work is done/Repairs completed a year ahead of schedule.** Repair work to the Arthur V. Watkins Dam around Willard Bay was declared finished this week, a year ahead of schedule. That is good news for boaters who use Willard Bay. Since the dam sprang a leak two years ago, Willard Bay has had such low levels that the south marina has been closed half the time and boating everywhere was severely restricted. Repair of the dam early is especially good news for the Weber Basin Conservancy District. Willard Bay is the district's single biggest storage area. When the dam sprang a leak, the district had to let 100,000-acre-feet of water, an amount equal to Pineview Reservoir, flow into the Great Salt Lake. Since then, the ability of the bay to store water has been cut in half. Repair of the leak involved fixing the whole dam so it would not leak again. The leak that sprang two years ago was due to that sandy soil, he said. Water seeping through the sand slowly "piped," digging its own channel, and finally came bubbling up on the outside of the dam's southeast corner. A year of testing found that the dam's structure was sound, but the ground under its entire south and southeast sections was all like beach sand, susceptible to more leakage and piping. The solution was to dig a ditch down through the dam, through the sand and into the clay underneath, then fill that ditch with a cement-bentonite wall. The result is a sort of dam within a dam, an impervious wall in the sandy subsoil locked to the clay.
Source: http://www.standard.net/live/news/149964/

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer